N3
Connecting Healthcare

N3 Network User Guide

Ref No:	N3SP-TEC-TRG-148
Version:	1.3
Author:	Ian Read
Date:	6 July 2010
Document Status	Issue

NHS

N3 managed on behalf of
the NHS by
BT

All information in this document is provided in confidence for the sole purpose of adjudication of the document and shall not be used for any other purpose and shall not be published or disclosed wholly or in part to any other party without BT's prior permission in writing and shall be held in safe custody. These obligations shall not apply to information which is published or becomes known legitimately from some source other than BT

Registered Office: 81 Newgate Street, London EC1A 7AJ

Document Information

This document is available in two forms, controlled and uncontrolled. The controlled variant is maintained electronically and accessed by authorised persons of the N3SP Document Library. Uncontrolled variants are all other electronic and printed copies.

Document Title	N3 Network User Guide		
Version	1.3	**Issue Date**	6 July 2010
Doc Ref	N3SP-TEC-TRG-148	**Security Classification**	
Review Date		**Controlled Release**	Yes
Doc Status	Issue		

Contents

1 Introduction

1.1 Purpose

This guide describes the technology and features of the N3 Network.

N3 is the private wide area network for the UK National Health Service (NHS) in England and Scotland.

1.2 Readership

The guide is primarily for NHS organisations that are N3 network end-users. It will also be useful to:

- people in management organisations such as:
  - NHS Connecting for Health (NHS CFH), Strategic Health Authorities (SHAs) and Primary Care Trusts (PCTs) in England
  - NHS NSS (National Services Scotland) and Health Boards in Scotland
- third-party companies and organisations providing services to the NHS using the N3 network.

1.3 Scope

The guide includes:

- N3 Overview – of the network and its purpose. This can be read alone for a quick understanding of N3.
- Network In Detail – a technical guide
- Network Security – security measures and responsibilities
- Capacity Management – monitoring/reporting and core capacity
- How To guide – contacts and processes

1.4 Disclaimer

The document is provided by N3SP for advice and guidance. It is not part of any contract requirement, agreement or understanding. Policy and other factors may have changed since this guide was published. Definitive and up-to-date policies and procedures are available from NHS CFH in England and NSS in Scotland.

2 N3 Overview

2.1 History

The N3 network began in England in April 2004.

The previous NHS private data network in England and Scotland was called NHSnet. NHSnet was jointly run by BT – branded as HealthNet and Cable & Wireless – branded as NHSnet.

Most NHS organisations and locations were already NHSnet end-users and were migrated across to N3. N3 was provided as a 'broadband' network. Lower speed eg: ISDN NHSnet connections were upgraded to broadband (DSL) speed when they were migrated. Most large NHS sites received high bandwidth Ethernet-based services. All N3 services were allocated using the National Allocation Algorithim (NAA) rules in force at the time.

The N3 network in Scotland began in April 2005. New core POPs were created to cover Scotland. This provided connectivity to the N3 network in England N3SP

NPFiT (National Programme for IT) in England – now NHS CFH (Connecting for Health) – appointed BT as the N3 Service Provider (N3SP). In practical terms this means BT provides and manages the N3 network as a network integrator; using data network services from all public data network operators – to give best value to the NHS.

N3SP's initial contract to run N3 in England is until the end of March 2011. NHS CFH can optionally extend the contract and have recently confirmed they will do this, for a further two years – until the end of March 2013.

The services N3SP provide are divided into:

- Foundation Services – core infrastructure services
- Catalogue Services – user access services

N3SP was appointed by National Services Scotland (NSS) to extend N3 into Scotland in early 2005. The Scotland N3 contract also ends in March 2011, with a separate option to extend.

2.2 Purpose

The original stated purpose of N3 was to connect NHS organisations – at broadband rate or greater – to National Applications.

2.2.1 National Applications

Originally these were:

- Choose and Book - online appointment booking accessible by patients and clinicians
- Electronic Prescribing – electronic transmission of prescriptions to pharmacies
- Electronic Patient Record – centrally held clinical record, accessible throughout the NHS

The following are also important initiatives, with their applications relying on N3 connectivity;

- NHSmail – personal 'for life' (@nhs.net) email addresses and mail system
- (England) GPSoC – a number of initiatives including
  - integration of GP clinical systems with Electronic Patient Record
  - options to switch from surgery to data-centre based/remotely accessed systems.
- (Scotland)
  - Emergency Care Summary (ECS)
  - SCI Gateway – for integrating primary and secondary care

Some of the functions of PACS – the systems for electronic storage/transfer/viewing of diagnostic images (x-rays and scans etc) – also rely on N3 connectivity.

2.2.2 Ownership

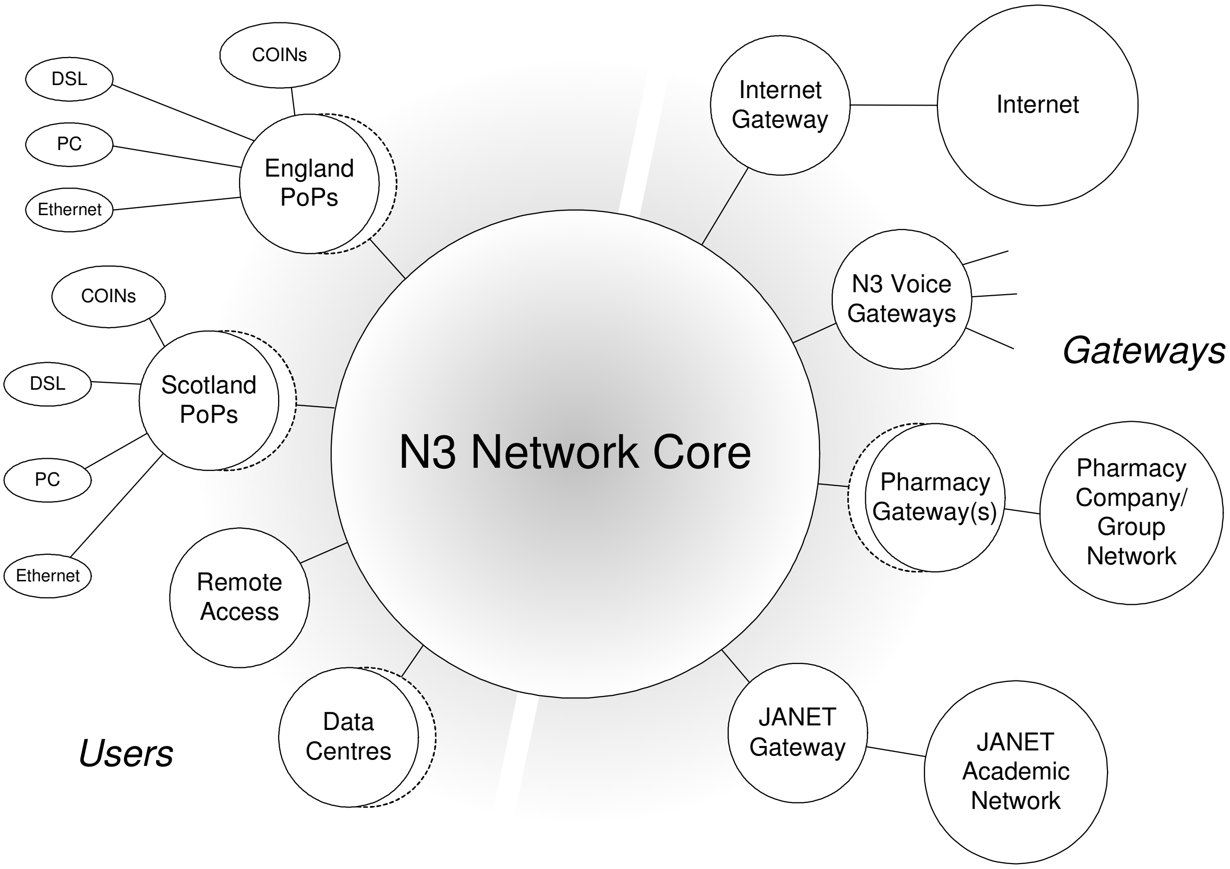
The N3 network is "owned" by NHS CFH in England and NSS in Scotland. These organisations are responsible for:

- setting policies for
    - security/access
    - IP addressing (See 3.1)
    - QoS (See 3.2)
    - DNS (See 3.3)
- managing
    - IP addressing
    - DNS naming
    - the capacity of the network core.

2.3 Overview/Diagram

N3 is an Internet Protocol (IP) network; the same type of networking used on the Internet and now almost universally used to connect computers and other systems. It's a Wide Area Network (WAN), connecting many different sites across the NHS within England & Scotland.

Below is an overview diagram of the N3 network, the N3 users and the other networks that connect to it. It shows N3 conceptually rather than exact connections. For instance there are many PoPs (Points of Presence) and several gateways, some of which actually connect via PoPs.



N3 is based on 57 PoPs in England and 5 PoPs in Scotland. They are the local points where individual end-user access (so-called “Catalogue”) services are connected to N3. The PoPs give the network its reach and also make it easier for different operators to be used for the access services.

Until recently the PoPs were joined together by a core network based on BT's Metroflex Multi Protocol Label Switching (MPLS) data networking service. A new core network is now in place in England. It is based on high-speed Ethernet data networking services from Virgin Media and BT (Etherflow). It will broadly double the England network core capacity for the same cost as the current MPLS core.

See 5 Capacity Management for more details.

2.4 Access (Catalogue) Services

N3 user access connections are known as *Catalogue Services*, as they’re ordered from a defined/agreed catalogue. There are a wide range of catalogue services for the different sizes and needs of NHS organisations. The catalogues for England and Scotland are similar.

N3SP has to review all catalogue services at least once every two years, to ‘refresh’ the catalogue – making sure it reflects technology advances and/or cost reductions. However users may generally opt to stay on existing services.

2.4.1 End User Services

There are three main categories:

- ADSL Broadband Services - for small sites (up to 8Mbps downstream and up to 832kbps upstream)
- Private Circuit - for medium sites (up to 2Mbps “symmetrical”)
- Ethernet - for large sites (10Mbps – 100Mbps)

There are also remote secure access services for mobile / remote or occasional NHS users.

2.4.2 Data Centre Services

Data Centre connections are a special type of catalogue service. Data Centres host applications and so serve many end-users, making them focal points for a lot of data traffic. Therefore they are connected directly into the N3 core, in the same way as a PoP. They are typically 100Mbps+ services with the potential to go up to 1Gbps.

2.5 Security

N3 security requirements mean each end-user connection should have a firewall between an organisation’s local network(s) and computers and the N3 network, to control what data can go back and forth. For small site services – normally for GP practices or similar – the firewall is provided/ built into the router that terminates the N3 at the site. All NHS end-users are connected to N3 on the understanding they conform to:

- in England, the Information Governance Statement of Compliance (IGSoC). Details can be found at: http://www.connectingforhealth.nhs.uk/systemsandservices/infogov/igsoc.
- in Scotland: the Code of Connection.

Although N3 is a private and secure network, data passing across N3 is not encrypted as standard. The exceptions to this are:

- The N3-12-4 Extended IP VPN Catalogue service which encrypts traffic across the Internet and then across N3 to a specific site.
- The N3-12-x Main-To-Branch connection services which encrypt traffic across N3 between GP practice sites.

The sender and receiver of sensitive data are responsible for their data's security on N3. In practical terms this normally means building security and encryption into individual applications (as with the National Applications listed in Section 1.1.1.).

4) Network Security describes security measures in place and users' responsibilities.

2.6 Core/Foundation Services

2.6.1 Core/PoP Bandwidth Policy

The original stated purpose of N3 was to connect NHS organisations – at broadband rate or greater – to National Applications in England (see 1.1.1). It was introduced for similar reasons into Scotland.

N3 is also the de-facto NHS Wide Area Network (WAN) in England and Scotland, used for other purposes, such as connecting to:

- supplier applications (for example for purchasing)
- other (non-strategic or local business or clinical applications)

These connections could be across the N3 network to another N3 user or they could be to Internet destinations via the N3 Internet Gateway or via other interconnect services e.g. JANET, NHS Wales and soon the Government Connect network.

The N3 network core is the shared part of the network. NHS CFH and NSS are responsible making sure the bandwidth of the connections between individual PoPs and the inner part of core are adequate for a PoP's users to support national and business critical applications for the NHS – realistically this means adequate for most of the demands at most times. N3SP are responsible for ensuring the inner part of the core is adequately sized.

- Capacity Management – N3SP provide comprehensive weekly and monthly usage reports and makes recommendations for upgrades and downgrades, based on trigger points specified in an agreed capacity management policy.
- QoS (Quality of Service) Prioritisation – a technical feature of the N3 network that prioritises some data traffic when a part of the network is working near or at its maximum data-rate. The de-prioritised traffic may be delayed and/or discarded. *See below.*

2.6.2 Network Use & QoS

The data traffic on the N3 network is divided into the following types, so QoS knows how to prioritise it.

QoS Label	**Data Traffic Type**	**Used for**
EF	Voice over Internet Protocol	VoIP telephony
AF3	National Applications	interactive application traffic. eg: Choose & Book
AF4	Media Streaming	video conferencing
AF2	Community Applications	'local' applications
AF1	Bulk Data Transfer (for National Applications)	message or data transfer applications eg: PACS images, NHSMail
DE	Default (all other Traffic)	includes any Internet-bound traffic

For more details on QoS on the N3 network see 3.2. QoS.

2.6.3 DNS

The DNS (Domain Name System) allows IP network users, such as those on N3, to use (easier) alphanumeric aliases in place of numeric IP addresses. N3SP runs this vital piece of network infrastructure centrally for all N3 end users.

For more details see 3.3 DNS.

2.7 COINs

Community of Interest Network (COINs) are networks for local NHS communities. There are now around 66 COINs connected to N3, covering about 1/3 of connected sites. Local data traffic can stay within a COIN, which reduces the data traffic on the main N3 network. Many individual NHS organisation connections into the main N3 network are replaced by one or two COIN gateways.

Some COINs are fully-managed by N3SP. In other cases N3SP manages the COIN gateways and the local NHS community manages its own COIN infrastructure.

2.8 Gateways

N3 has a number of gateways to other networks and systems to increase its use and value. The main gateways are:

2.8.1 Internet Gateway

The Internet Gateway does two equally important tasks. It's the:

- single aggregation and access point for all Internet-bound traffic from N3 users. By restricting the connection to the Internet to just one gateway protecting N3 is simpler and more effective.
- firewall that protects N3 from the Internet, making sure that whilst N3 users can get onto the Internet, no Internet user can get onto N3.

2.8.2 Pharmacy Gateway(s)

In England the large number of pharmacy connections are aggregated and joined to N3 via a small number of gateways. The gateways limit access to N3 to what's needed for Electronic Prescribing, acknowledging the lower network and computer security at most community pharmacies.

2.8.3 JANET Gateway

The gateway to JANET – the UK university private network – allows doctors and healthcare professionals, particularly in teaching hospitals, to access this network from their N3 connected devices.

2.8.4 NHS Wales & NHS NI Gateways

NHS Wales runs a separate private data network but NHS Wales and N3 users can interconnect via this gateway.

There is also a gateway connection to the NHS network in Northern Ireland.

3 Network In Detail

3.1 IP Addressing

N3 is an Internet Protocol (IP) Network.

Each node (user/computer) on an IP network has a unique *IP address*. IP networks divide data into *packets* to send and receive. Each packet includes the *source* IP address where the packet came from and the *destination* IP address where it is going to.

A message or transaction, known as a *session*, is normally made up from a string of data packets. IP networks are packet switched. Individual packets can travel by more than one route if available, to their destination. If they arrive out-of-order they are reassembled in the right order, using unique serial numbers also sent in the individual packets.

N3 is an IP version 4 (*IPv4*) network. IPv4 networks have IP addresses normally shown in an x.x.x.x format, where x is between 0 and 255. For example 192.168.0.1.

3.1.1 Policy

N3 IP addressing policy is ultimately controlled by NHS CFH, although day-to-day IP address assignment is devolved to N3SP, the service provider for the N3 network. N3SP has devised an IP addressing scheme based on NHS CFH's IP addressing policy, to ensure the IP addresses allocated are *routable* on (usable across) the N3 network.

IP addressing policy is controlled by NSS in Scotland.

NHS CFH or NSS will arbitrate if there are any IP addressing use disputes between NHS organisations.

3.1.2 Address Ranges

The bodies that control the Internet and addressing standards on IP networks have agreed certain ranges of IP addresses to use in private networks. This means they're not recognised and switched (routed) across the Internet, so they can be used on any number of times on private networks, when the private networks are connected to the Internet.

N3 uses the following private IP address ranges (space):

- All of Class A: 10.0.0.0 -10.255.255.255
- Part of Class B: 172.17.0.0 - 172.31.255.255
  (used by GP connections in England for N3's predecessor network NHSnet and retained for N3)

The Class C address space for private networks, 192.168.0.0 - 192.168.255.255, is not even routed across the N3 network. It's reserved and recommended for individual NHS organisations to address their own Local Area Networks (LANs). Network Address Translation (NAT) is used to convert these internal IP addresses to the external IP address(es) assigned to individual NHS organisations connecting to N3.

The 164.134.0.0 – 164.134.255.255 address range is used in Scotland and is routed across N3.

In a similar way to the above, many N3 IP addresses are summarised and translated using NAT at the Internet Gateway. This means all Internet traffic from N3 comes from a small range of registered IP addresses.

3.1.3 Legacy RIPE vs Private Addressing

Early on in the history of the Internet and IP networks the NHS was assigned a range of Internet registered IP address from the European IP address registry - RIPE. These were used extensively for

NHSnet, the predecessor network to N3. This was before private addressing ranges were agreed and Network Address Translation was widespread.

It was NHS policy to develop a compliant private addressing scheme for N3 and its other networks:

- NHS organisations using registered RIPE IP addresses within N3 were expected to migrate to the Class A private address range IP addresses assigned by N3SP; using NAT and Class C private addressing on Local Area Networks wherever possible. Most organisations have now done this, except where there were special circumstances.
- Any new or existing Community Of Interest Networks (COINs) recognised by the Connecting for Health will have their IP address allocation managed by N3SP.
- Organisations who were already allocated IP addresses from the Class A private address range for NHSnet (by BT HealthNet or Cable & Wireless) have generally retained these for use on N3.
- Independent implementations of the Class A private addressing are not permitted on N3.

Any registered addresses released are returned to RIPE (Reseaux IP Europeens).

3.1.4 VoIP Ranges

Where NHS organisations are deploying voice solutions, it is good practice to use separate Virtual Local Area Networks (VLANs) for voice and data traffic. This reduces the voice system's vulnerability to attack from personal computers (PCs), for example to eavesdrop or to deny service to the voice applications.

To support NHS organisations N3SP allocates separate IP addresses for sending/receiving VoIP traffic across N3, for use with Voice VLANs. They are allocated from specific ranges from the Private Class A address space (10.0.0.0 -10.255.255.255) and reserved for voice use only

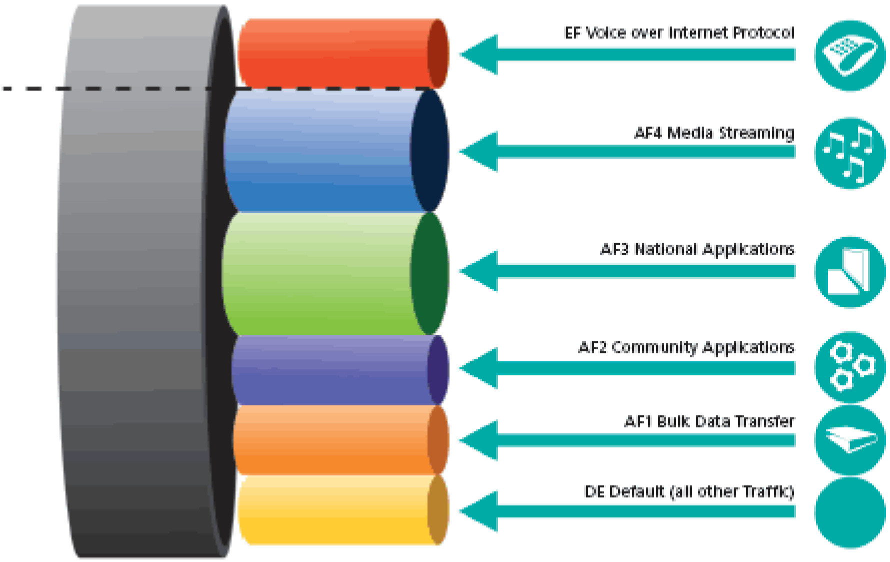
Any NHS organisations that wish to use the N3 network to carry voice traffic must submit their VoIP addressing requirement to N3SP using the N3 IP addressing request form. The size of address range(s) allocated will be based on the number of VoIP telephone handsets anticpated.

3.1.5 Requesting IP address ranges

IP Addressing Requests > See How To for details.

3.2 QoS

The N3 Network has a 6 layer QoS (Quality of Service) solution. The diagram below shows the set-up. The grey pipe is the overall bandwidth available for a given part of the network. Each QoS class of traffic has a priority and a *contracted bandwidth* - a percentage of the overall bandwidth (data rate), shown by the smaller coloured pipes. When the network or parts of it are *congested* – operating close to or at maximum bandwidth – QoS decides how traffic is handled.


EF Voice over Internet Protocol
AF4 Media Streaming
AF3 National Applications
AF2 Community Applications
AF1 Bulk Data Transfer
DE Default (all other Traffic)

The *EF* (Expedited Forwarding) class is used for VoIP telephony – its contracted bandwidth is only ever a small percentage of the overall bandwidth and can't be exceeded. This makes sure it's always available. However *AF* (Assured Forwarding) and *DE* (Default) class traffic can *burst* into any spare capacity when the network's not congested – including any unused EF capacity. AF traffic has priority over DE traffic when the network's congested. The AF *sub-classes* (*AF1/2/3/4*) all have equal priority, however they can have different contracted bandwidths depending on expected traffic. Although the diagram shows AF4 and AF3 with larger contracted bandwidths it's just an example. AF sub-class contracted bandwidths can be set at any value.

Even if the network is fully congested – with traffic occupying all the bandwidth – all traffic will still be passed, as long as the traffic in each QoS class is no more than its contracted bandwidth percentage. However when the network is near or fully congested and traffic in any of the AF or DE classes exceeds its contracted bandwidth, then it's likely to have some of its data packets *discarded*. This packet loss will be worst for DE – the lowest priority – traffic. Where the traffic is using TCP protocols it can recover from missed packets by attempting to resend them. With TCP, as long as there aren't too many missed packets, an end-user or process may only see a slow-down in performance rather than outright failure.

QoS works 'end-to-end' – ie: from one end-user's N3 router to another across the N3 network. For QoS to work data packets must be *marked* (*tagged*) so the network between knows what class they're in. Marking is added/removed at the N3 user routers.

NHS CFH and NSS set the mix of contracted bandwidth percentages for the N3 Network, known as *QoS Profiles*. They've also specified the intended use for each class/sub-class, as shown on the diagram. Profiles are deliberately different on different types of N3 access (catalogue) services and across the N3 network core, based on the traffic mix expected. Scotland's core QoS profiles may differ from England's. NHS CFH have clearly stated their focus is on traffic in AF1 and AF3 used for National Applications - Choose & Book, Electronic Patient Records, Electronic Prescribing plus PACS, NHS Mail and GPSoC GP applications. For these applications AF3 is used for interactive traffic and AF1 is used for bulk transfer eg: PACS images. All Internet-bound traffic is sent as DE.

Note: Around 1% of overall bandwidth is typically needed for QoS management, so this must be factored into any QoS profile – see the actual profile examples below.

3.2.1 QoS Profiles

Two examples of the current profiles.

Remember: "*Profiles are deliberately different on different types of N3 access (catalogue) services and across the N3 network core, based on the traffic mix expected.*"

N3 Core Network QoS Profile (PoP <> Core)	
Class	*% of CDR*
EF	10%
AF1	5%
AF2	7.5%
AF3	30%
AF4	7.5%
DE	39%
Management	1%

3.2.1.1 N3-2-56 – 10M Ethernet (with DSL backup) QoS Profile	
Class	*% of CDR*
EF	10%
AF1	1%
AF2	14%
AF3	50%
AF4	10%
DE	14%
Management	1%

N3-2-56 is the catalogue/access service used to connect small/medium sites. The profile is shown is for the Ethernet primary.

3.2.2 QoS Profile Refresh

N3SP works with NHS CFH and NSS to ensure QoS Profiles are adjusted to make best use of the N3 network, as the mix of traffic does change with time. Typically these checks and changes are done yearly, to adjust the profiles to reflect current and forecasted requirements.

QoS Profile Refresh Feedback > See How To for details.

3.3 DNS

3.3.1 Why DNS?

The DNS (Domain Name System) allows IP network users to use (easier) alphanumeric aliases in place of numeric IP addresses.

A user typing *www.nhs.uk* into a web browser will get to the website hosted by a server at Internet IP address 217.64.234.65. DNS tells the user's computer that *www.nhs.uk* is actually at IP address 217.64.234.65. The user's computer, the server hosting the website and the network on their own only understand IP addresses.

DNS also lets network and application providers move servers and services to different IP addresses invisibly, whilst keeping the DNS naming the same for users.

3.3.2 nhs.uk

nhs.uk is the recognised and registered Internet domain for the UK National Health Service on the public Internet – used for instance when an NHS organisation wants a public website. However the NHS also uses nhs.uk on N3 and its other private networks. An N3 user typing *nww.nhs.uk* into their browser will get the *internal* NHS top-level website hosted and accessible on the N3 network only. If they type www.nhs.uk though they'll get the public (*external*) top-level website on the Internet. The user can get to the public Internet from N3 because the network has a gateway to the Internet, but it's a different website on a different network.

Using nhs.uk both *internally* and *externally* (on the Internet) makes the user experience seamless, although the internal and external DNS are actually separate *realms*, that happen to use the same naming. The internal realm could have used different domain naming – for instance *nhs.n3* or *nhs.private*.

nhs.uk is the NHS's top level domain. Individual NHS organisations normally have their own *sub-domain* of nhs.uk, for example: *connectingforhealth.nhs.uk*. Sub-domains are normally just called domains, when they're being talked about alone. A full DNS address (technically known as a Uniform Resource Locator "URL") includes the hostname prefix - the name of a server where a website or other service is hosted. For example *www.connectingforhealth.nhs.uk* identifies the web server on the public Internet called 'www' belonging to the *connectingforhealth.nhs.uk* Internet (sub!) domain.

NSS uses and administers *.scot.nhs.uk* specifically for Scotland.

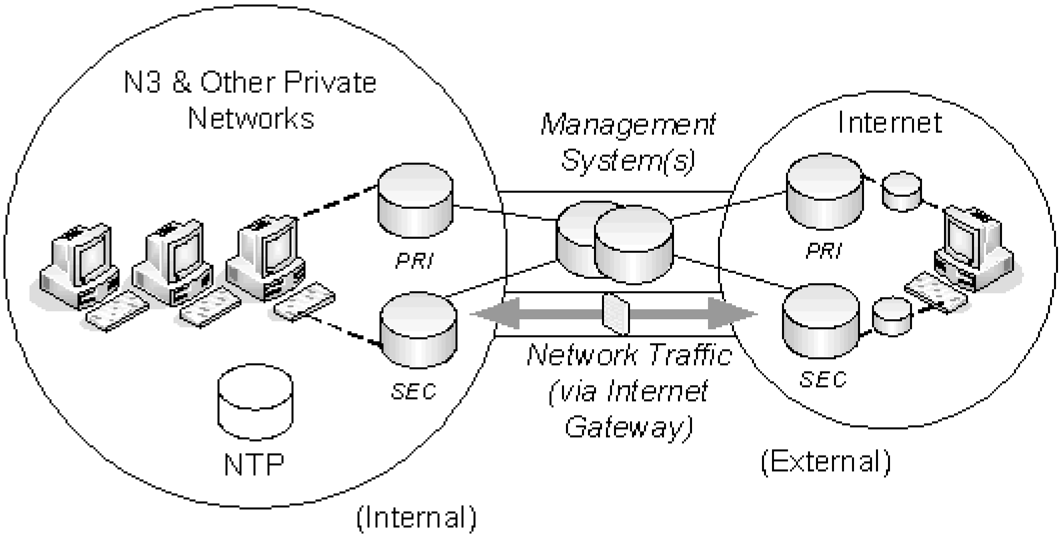
3.3.3 How DNS works

DNS works by user (*client*) computers sending queries (requests) to a local *DNS server* to get the IP addresses they need. This is called *resolving*. Domain name data is distributed and/or delegated amongst a number of name servers. Often the local name server doesn't hold all the data requested, even though local servers do store (*cache*) some answers to recent DNS queries. If the answer isn't cached, the local server checks with other name servers to get the data. This is known as *recursive* operation. This process continues until the definitive DNS information (*record*) for a domain is found on an *authoritative* DNS server. Although previous examples have used the *nhs.uk* domain, the resolving process works for queries about any domain registered and in use. An N3 user DNS request for the IP address of *www.bt.com* would be resolved in a similar way.

Because DNS is so important there should always be at least two DNS servers for any domain, for resilience. These are often called *primary* and *secondary*, although they often share DNS requests more equally than the names suggest, depending on how they're set up.

3.3.4 N3/nhs.uk DNS setup

N3SP provides central nhs/uk DNS server setups for both internal and external (Internet) use, as shown in the diagram below.


N3 & Other Private Networks
Management System(s)
Internet
PRI
SEC
PRI
SEC
Network Traffic (via Internet Gateway)
NTP
(External)
(Internal)

NHS CFH, NSS and N3SP recommend that all N3 users use the N3SP provided internal DNS servers shown as their ‘local' servers for DNS queries. They are at ‘well-known’ N3 network IP addresses , that can be confirmed by NHS CFH or NSS on request.

N3SP also provides a Network Time Protocol reference (NTP) source for N3 users to synchronise the clocks in servers and PCs to. Although NTP is shown separately in the diagram, the reference source is actually at the same IP addresses as the internal DNS service above.

3.3.5 DNS Records

Data for a domain, such as nhs.uk, is arranged in *zone* data files with a number of (*resource*) records. The most often set-up and used are the:

- *Address Record (A-record)* - used to direct users to live servers for web browsing, file transfers, etc.
- *Mail eXchange Record (MX-record)* - used to direct messages to email/messaging servers for a domain

Other types of record also used on the nhs.uk DNS servers are:

- *Start of Authority (SOA):* Defines the start of a zone data file. It includes information on the name server with ultimate authority for the domain and who to contact about the domain
- *Name Server (NS):* Defines one or more name servers with definitive DNS information
- *Canonical Name/Alias (CNAME)*: Defines additional aliases for an IP address (as alternative to multiple A records).
- *Pointer (PTR*): A ‘reverse lookup' record - associates an IP address to a DNS name; effectively the reverse of an A record.

3.3.6 DNS Change Requests

From time to time network users need to change DNS records – to create/amend/delete new zone files and/or the records within them.

nhs.uk DNS records are owned and administered by Connecting For Health. NSS in Scotland administers the *scot.nhs.uk* (sub) domain.

DNS Change Requests > See How To for details.

4 Network Security

N3 is a very large network, with 1.3 million NHS end-users and over 40,000 connections in England and Scotland connected to regional Points of Presence (PoPs). A high speed any-to-any core based on Ethernet connects the N3 PoPs. There are at least twelve major data centres connected directly to the MPLS network to provide national and local services and applications. Two additional data centres provide authentication and access profiling.

The network has a wide variety of end-user NHS organisations from GP practices to large hospitals with dedicated IT staff. It has gateways to other networks, most notably the Internet. A number of approved NHS suppliers are connected to N3.

All involved have security responsibilities:

- the network owners - NHS Connecting For Health and NHS National Services Scotland who set security policy, rules and requirements.
- the service provider - N3SP by ‘building-in' network security through design and operation
- the end-users - anyone who connects to and uses N3 by acting responsibly, following NHS Connecting for Health and NHS Scotland policy and rules and maintaining good security practices

4.1 General Security

The N3 network is a private data network designed to ensure:

- Confidentiality with physical and logical restrictions to network access
- Integrity with authorised user access
- NHS organisations and approved third parties only can connect. Third party access is normally restricted in terms of types of network traffic and N3 destinations.
- Availability with resilience and fallback built into the core network design and access (catalogue) services. The level of resilience at an end user site depends on the Catalogue Service in use

Data sent across N3 is not encrypted (unless using the VPN N3-12-4 Catalogue service which encrypts traffic across the Internet and the N3 network to a specific site). As with any data network there is a risk that data can be intercepted. There are number of security factors that minimise the chances of this happening, including:

- physical and organisational security of the core network, data circuits and end-users’ equipment
- N3SP service level agreements/contractual agreements to ensure secure network operation
- established policies, rules and in some cases laws to control user behaviour

4.2 Physical Security

N3 PoPs and Community of Interest Network (COIN) gateways are in physically secure BT premises. N3SP equipment cabinets have the additional security of a remote locking and unlocking solution. This ensures only authorised personnel can access the cabinets following request and authorisation from the N3 Operational Support helpdesk. Alarms are generated if unauthorised entry is attempted or an unusual condition or problem is detected. This allows the N3 Operational Support helpdesk to carry out an investigation

4.3 Patient/Sensitive Data

Data transmitted across N3 is not encrypted by the network (unless using the services mentioned in 2.5 Security. The network alone is not secure enough to meet Caldicott Guidelines requirements – for transmitting patient identifiable or similar sensitive data. Therefore the sender(s) and receiver(s) of such data are jointly responsible for implementing a solution that conforms – not NHS Connecting for Health, NHS National Services Scotland or N3SP.

The normal practical solution is to encrypt application data where it traverses N3 between users and application providers. The encryption method must meet Caldicott Guidelines requirements.

Access to National Applications (as listed in 1.1.1) is thereby encrypted to meet these requirements.

4.4 Network border security - firewalls

The core of the N3 network is protected from individual end-users and vice versa by firewalls, devices that only allow certain types of IP data to pass. Firewall rules control what types of IP data packets can pass. Firewalls are also used to protect N3 at its gateways to other networks. All of these firewalls are mandatory.

Firewalls are often used to protect a small network where it connects to a larger network; such as a GP surgery LAN (Local Area Network) to the N3 Wide Area Network. The firewall passes data in both directions to make the connection useable, but it will only do this if the session (streams of data traffic back and forth to complete a task, such as browsing a web site) is started by a user/device on the small network. In this way firewalls protect the user's local network from users on the larger network they're connected to.

For GP and similar lower-speedN3 catalogue (access) services, the firewall is within the router that terminates the N3 connection at the user's premises. Users with these types of service can request changes to the standard firewall rule set configured by N3SP on the router to meet local needs.

GP Firewall Rule Changes > See How To for details.

Larger NHS sites and organisations use N3 catalogue (access) services where the firewall is not built into the terminating router. They must deploy their own compliant firewall between N3 and their local network, in line with NHS CFH and NSS security rules. They are responsible for managing and configuring their own firewall rules.

Firewalls are also used at the N3 gateways to other large networks to control what passes between the networks:

- The Internet Gateway firewall rule set controls N3 user access to the Internet. The rule set has evolved to meet NHS business needs and is controlled by NHS Connecting for Health. End-users must contact NHS CFH (or NSS in Scotland) with any Internet Gateway rules change requests.

  Internet Gateway Firewall Rule Changes > See How To for details.

- NHS Connecting for Health and NHS National Services Scotland also set the firewall rules for other N3 gateways. These include:
  - NHS Wales and NHS Northern Ireland networks
  - pharmacies and procurement networks
  - Social Services
  - government departments
  - NHS suppliers

4.5 Anti-virus/Anti-worm/Denial Of Service Attack Measures

N3SP is responsible for the security of the N3 network infrastructure such as routers, firewalls and DNS servers.

N3SP monitors the network using a number of methods for unusual activity that may indicate virus or denial of service activity. N3SP will investigate such activities and will alert NHS Connecting for Health and NHS National Services Scotland. N3SP will request that NHS Connecting for Health and NHS National Services Scotland contact the affected or offending end-user to apply appropriate fixes.

General Disclaimer

NHS CFH, NSS and N3SP will make every reasonable attempt to prevent any malicious data traffic from entering the N3 network. However it is not possible to monitor and verify all data traversing N3 due to the sheer volume of traffic. Network performance would also be significantly degraded if this took place. A significant proportion of the data passed over N3 is encrypted to protect patient data confidentiality. This prevents virus and worm detection. N3 users are therefore responsible for ensuring that their own systems and data are well protected. Below is a checklist to help with this.

4.6 User Security Checklist

Important network and data security responsibilities for end users (organisations and individuals):

- Ensure physical security of
  - site computer systems
  - N3 terminating router etc on site
- Ensure up-to-date PC protection
  - anti-virus and anti-worm
  - Spyware and Malware
- Ensure the N3 connection is
  - only used in conformance with the N3 access agreement
  - used in conformance with NHS Connecting for Health Information Governance guidelines
  - only used in line with local organisation operating procedures
- Ensure strict but practical access control
- Monitor use of the N3 network through organisational compliance programmes
- Ensure staff vetting and information security training and awareness procedures are in place
- Where there is no firewall protection provided or it has been removed from the N3 router at customer's request, the end user is responsible for the management and security of their own firewall which has been approved by NHS Connecting for Health Information Governance.
- Ensure that all borders are disabled or safe e.g. wireless LAN, Bluetooth, modem links, alternative ISP connections. Good practice guidelines can be viewed on the NHS Connecting for Health intranet site, accessible via the N3 network.
- Ensure that all router/hub/switch ports and other access points are closed/locked down to prevent unauthorised access.
- Protect any data against malicious or accidental loss. N3SP and the N3 network owners are not responsible for data loss, unless it is due to shortcomings in the design or implementation of the network.
- Ensure a local security policy is implemented, including the use and security of removable media, Internet access/use.
- Secure Patient Identifiable Data within local and remote applications to Caldicott Guideline standards
- Carry out appropriate and robust compliance security checks for current or potential sub-contractors

This checklist summarises good security practice. It does not supersede or replace local or national NHS security policies and guidelines.

Up-to-date NHS CFH Information Governance (IG) policy, guidance and resources are available on the CFH website: http://www.connectingforhealth.nhs.uk/systemsandservices/infogov

4.7 Internet Gateway Blocking

Relatively few Internet destinations are blocked at the N3 Internet Gateway. It is the responsibility of individual NHS organisations to further block destinations in line with their local Acceptable Use Policies for N3 and Internet use.

However sites defined as inappropriate by the Internet Watch Foundation are blocked at the N3 Internet Gateway. This block has been in place for some time.

A block on gambling sites became effective on 2 April 2008, with the most prevalent gambling sites used through N3 being blocked. All blocked sites will display a blocking message when they are accessed from within N3.

5 Capacity Management

N3SP provides historical usage (‘capacity') reporting for all live end-users who are directly connected to N3*. Data is collected regularly from N3 routers at end-user sites. HSCR (High Speed Customer Reporting) then aggregates the data and produces data tables and graphs showing usage, as a percentage of the maximum possible data rate a service can operate at.

* Where an end-user is part of a COIN and connects to N3 via a COIN gateway rather than directly, monitoring capability depends on the hardware in use and how the COIN’s managed

5.1 N3 Service Portal

Service reporting within the N3 Service Portal gives customers a detailed view of the performance of the service and network elements of their N3 connections.

The reports are generated by a BT system called High Speed Customer Reports (HSCR) which has been tailored for N3 requirements. HSCR generates textual and graphical performance reports based upon N3 network router information.

There are two types of report Dashboard and Customer Reports. Reports are generated based on profiles defined by groups of network devices (routers).

The N3 Service Portal can also be used to track the progress and resolution of incidents. The N3 Helpdesk incident tracking system regularly updates the service portal with this information.

5.1.1 User Account

N3 Service Portal Account/HSCR Access > See How To for details.

5.2 HSCR

HSCR produces automatic standard format weekly and monthly reports in Microsoft Word or PDF format. HSCR has a self-service web interface where users can – depending on their profile and type of service:

- download historic PDF reports
- set-up and run HSCR near real-time and historical usage reporting

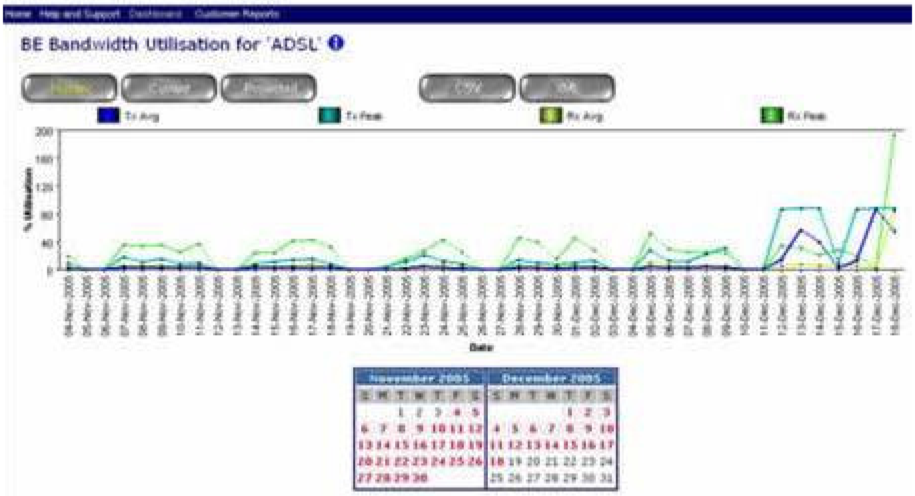
Below is an extract from a typical HSCR report:

Device	Interface Description	Tx KBytes	Tx Util (%)	Tx Busy Hr Util (%)	Tx Busy Hr/Date	Tx Peak Util (%)	Rx KBytes	Rx Util (%)	Rx Busy Hr Util (%)	Rx Busy Hr/Date	Rx Peak Util (%)
SIN0001----2-13	ATM 0/0	0	0.00	0.00	N/A	0.00	45,687	0.05	0.05	07:00/07	0.05
	Serial 0/0	7,245,119	1.49	42.51	14:00/30	42.51	12,100,469	2.48	59.93	09:00/22	59.93

	Serial 0/0.101	7,240,078	1.12	31.05	09:00/14	31.05	12,093,355	1.88	32.50	09:00/22	32.50

This report shows usage statistics for a single N3 site. The site here has a 2Mbps serial connection as primary and an ADSL line as secondary connection (shown here as ATM0/0).

Here is an example of a on-demand graphical report. It shows the bandwidth used as a percentage of maximum capacity/data rate.



HSCR can also provide statistics on each QoS class against the contracted bandwidth for that class (see Section 4 for further explanation of QoS). Because QoS guarantees each class of traffic a minimum reliable (contracted) bandwidth, whilst allowing other traffic to burst into any unused bandwidth, QoS reports showing > 100% of the contracted bandwidth in use is normal.

5.3 N3 Network Core Capacity

The N3 network core is the shared part of the network. NHS CFH and NSS are responsible for making sure the bandwidth of the connections between individual PoPs and the inner part of core are adequate for a PoP's users. Realistically this means adequate for most demands at most times. It does not mean providing a core capable of being used simultaneously by all end-users at their maximum possible rates; which is in effect over-providing. N3SP are responsible for ensuring the inner part of the core is adequately sized regardless.

Quoted bandwidths for N3 Catalogue (access) services are guaranteed for the end-user site to N3 PoP part of a connection only.

N3SP provides a comprehensive monthly capacity reporting package to NHS CFH and NSS. It includes detailed utilisation data for N3 PoPs and for strategically important gateways and data centres known as Key Measures. It also includes a summary report with analysis and recommendations for upgrades and downgrades at agreed trigger levels, based on trends and other knowledge. Upgrades and downgrades to PoP to core connections are ultimately NHS CFH and NSS decisions, made against the background of jointly agreed capacity management policy

Results from 'speed tester' tools often do not give an accurate view of the speed/performance of individual N3 connections and/or the N3 network core:

- The N3 Speed Tester tool is for indicative speed (bandwidth/data rate) checks on N3 DSL access services only. It is not suitable for use with high bandwidth access services.
- Internet-based speed tester tools are not recommended. The 'round trip' measured by these will include not just the basic N3 network components, but also the N3 Internet Gateway and

the Internet connection to the tester's server. The performance of Internet connections is often unknown and almost always variable. There's also no guarantee on or knowledge of how well the speed tester software and the server at the far end are performing.

QoS (Quality of Service) is a valuable feature that enables available bandwidth to be managed and used as effectively as possible. When considering PoP to core connection upgrades, NHS CFH and NSS will focus on ensuring traffic in AF1 and AF3 QoS classes used for National Applications, is being passed across the PoP to core connection satisfactorily (ie: the number of packets discarded by QoS is not significant).

The aggregated core capacity in England has recently increased to 10Gbps with the migration to the N3 New Core. This figure is the total of all the individual PoP to core bandwidths plus the bandwidth of the aggregation points where most of the DSL services connect into the core.

6 How To

6.1 Request IP Address ranges

- England
    - New or additional IP Addresses request forms can be downloaded from http://www.n3.nhs.uk/files/documents/n3ipaddreqform.doc
    - All completed forms should be emailed to n3deliverytechteam@bt.com
- Scotland
    - Email to nisgtelecom.nss@nhs.net

All requests must be made on a site by site basis.

The lead time for an IP address allocation is normally five business days. This will depends on all required information being provided on the forms and the size of address range/space requested. Organisations that need large address space(s) for a major system deployment should ensure their plans allow enough time for the allocation process.

A request for Class A private addresses can be rejected due to one or all of the following reasons:

- It is too large based upon the organisation size
- It is not an efficient use of address space
- Insufficient supporting documentation for a large allocation request

If a request has been rejected the allocation request will be jointly reviewed by the N3SP Technical team and NHS CFH or NSS. A response will then be issued to the requester based on this review.

6.2 QoS Profile Feedback

- England: Email to n3@nhs.net
- Scotland: Email to nisgtelecom.nss@nhs.net

6.3 Request nhs.uk DNS changes

- England: For DNS Change Request forms and contact information click here: http://www.connectingforhealth.nhs.uk/systemsandservices/addressing/domainnames
- Scotland: For DNS Change Request forms, contact: nisgtelecom.nss@nhs.net

DNS Change Requests, to change either zone data files or individual DNS records, must be made directly to these bodies. N3SP cannot accept DNS Change Requests from end-users.

6.4 Firewall Changes

6.4.1 GP Firewall Changes

- England: Contact CFH Service Desk for details.
- Scotland: Email to nisgtelecom.nss@nhs.net

6.4.2 Internet Gateway Changes

- England: Contact CFH Service Desk for details.
- Scotland: Email to nisgtelecom.nss@nhs.net

6.5 N3 Service Portal Access

The Service Portal is a password protected online tool that you can access wherever and whenever you have internet access:
http://www.n3.nhs.uk/serviceportal/serviceportalaccessrequest.cfm

The Standard user profile gives access to

- My Portal
- N3 Application
- N3 News Portlet
- N3 Network Status .

The PCT user profile gives additional access to:

- High Speed Customer Reports
- Expedio Incident Management